UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NORTH DAKOTA

BEATRICE BYRNE, individually and on behalf of all others similarly situated,	)	
	)	Case No.
Plaintiff,	)	
v.	)	**CLASS ACTION COMPLAINT**
MEDSCAN LABORATORY, INC. D/B/A ADAPTIVE HEALTH INTEGRATIONS,	)	
Defendant.	)	

Plaintiff Beatrice Byrne ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Medscan Laboratory, Inc. d/b/a Adaptive Health Integrations ("AHI" or "Defendant"), a North Dakota corporation, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record.

I. NATURE OF THE ACTION

1. This Class Action Complaint (the "Action") addresses the recent targeted cyberattack against Defendant AHI that allowed a third party to access Defendant AHI's computer systems and data, resulting in the compromise of highly sensitive personal information belonging to hundreds of thousands of victims whose data was sent to AHI by various health-related entities (hereinafter, the "Data Breach). Because of the Data Breach, Plaintiff and hundreds of thousands of Class Members suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack and the imminent

risk of future harm caused by the compromise of their sensitive personal information, including Social Security numbers.

2. Information compromised in the Data Breach, according to the "Notice of Data Security Incident" sent by Defendant, includes: (1) full name, (2) address, (3) date of birth, (4) phone number and (5) Social Security number (collectively, the "Private Information" or "PII").[1]

3. Plaintiff brings this Action on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that they collected and maintained, and for failing to provide adequate and timely notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

4. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on AHI's computer system and network in a condition vulnerable to cyberattack.

5. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

6. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.,* opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's

[1] http://www.adaptivehealthintegrations.com/36-2/, (last accessed May 2, 2022)(hereinafter, the "Notice").

licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

7. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

8. Plaintiff and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

9. By her Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to AHI's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

10. Accordingly, Plaintiff brings this action against Defendant seeking redress for their unlawful conduct, and asserting claims for: (i) negligence, (ii) negligence *per se*; and (iii) unjust enrichment.

II. JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. §1332(d)(2). There are at least 100 putative Class Members, the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000 exclusive of interest and costs, and Plaintiff Beatrice Byrne and Members of the proposed Class are citizens of states different from Defendant – namely, Plaintiff is a Nevada resident and Defendant is a North Dakota corporation.

12. This Court has personal jurisdiction over Defendant AHI because Defendant AHI conducts substantial business in this District.

13. Venue is proper in this Court pursuant to 28 U.S.C. §1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District.

III. PARTIES

14. **Plaintiff Byrne.** Plaintiff Byrne is a Nevada resident located in the city of Fallon, Nevada. Plaintiff Byrne provided her Private Information to a medical services provider who uses Defendant's services.

15. **Defendant Medscan Laboratory, Inc. d/b/a Adaptive Health Integrations.** Defendant AHI is a North Dakota corporation located in Williston, North Dakota. Defendant AHI provides software, billing and revenue services to healthcare companies and doctors' offices.

IV. FACTUAL ALLEGATIONS

DEFENDANT'S BUSINESS

16. According to the Defendant, "Adaptive Health Integrations provides both LIS Software Services and Billing / Revenue Services for laboratories[,] [p]hysicians offices and related healthcare companies."[2] Defendant's "billing services are integrated with one of the largest and most cost-effective clearing houses in the country [which] allows for greater efficiencies in processing claims submission[s] and electronic claim remittance."[3]

17. Defendant's website has no privacy policy, is maintained on a WordPress blog, and misspells the name of the company (Adaptive is spelled as "Adapative") at the top of the website. There is no way for consumers to know what information is being collected about them, if that information is being kept secure, and if the Defendant is who they even say they are, given the

[2] http://www.adaptivehealthintegrations.com, (last accessed May 2, 2022).
[3] *Id.*

name on the website is misspelled. Little information is publicly available on the Defendant. In addition to there being almost no information on Defendant on Defendant's website, Defendant's Facebook page was seemingly deleted.

18. Plaintiff provided her PII to a healthcare provider which then passed that PII to Defendant in exchange for Defendant's services.

19. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

20. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

21. Plaintiff and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information.

THE DATA BREACH

22. Defendant's Data Security Incident Notice is woefully insufficient – it lacks critical information, including when Defendant was first aware of the existence of the Data Breach.[4] The Notice did not explain what type of cyberattack had occurred, what parts of Defendant's computer systems were affected, what type of information had been affected, or any of the other facts and circumstances surrounding the Data Breach.

23. Defendant states that, on or about October 17, 2021, an unauthorized third party accessed data stored on Defendant's systems.[5] After discovering the incident Defendant

[4] http://www.adaptivehealthintegrations.com/36-2/, (last accessed May 2, 2022).
[5] *Id.*

commenced an investigation to determine the full nature and scope of the incident and to secure its network. Defendant's investigation did not conclude for almost half a year – on February 23, 2022.[6] In that span of time, Defendant failed to notify the Plaintiff or members of the putative Class. Ultimately, the investigation concluded that the incident involved the unauthorized acquisition of PII.[7]

24. The investigation commissioned by the Defendant revealed that the PII accessed without authorization included: (1) full name, (2) address, (3) date of birth, (4) phone number and (5) Social Security number.[8]

25. Upon information and belief, and based upon the fact that notice was sent to affected consumers pursuant to North Dakota Century Code § 51-3-02, the Private Information contained in the files accessed by hackers was not encrypted.

26. Upon information and belief, the Data Breach was targeted at Defendant due to its status as a healthcare-related entity that collects, creates, and maintains PII.

27. Upon information and belief, the targeted Data Breach was expressly designed to gain access to private and confidential data, including (among other things) the PII of the Plaintiff and the Class Members.

28. Because of the Data Breach, data thieves were able to gain access to Defendant AHI's IT systems and compromise, access and acquire the Private Information of Plaintiff and Class Members.

---

[6] *Id.*
[7] *Id.*
[8] *Id.*

29. Due to Defendant' AHI's inadequate security measures, Plaintiff and the Class Members now face an increased risk of fraud and identity theft and must deal with that threat forever.

30. Despite first learning of the data breach in October 2021, notice to Plaintiff and Class members was not sent out until April of 2022, approximately six months after the Data Breach, Defendant first learned of this Data Breach. Defendant's delay in notifying its customers affected by the Data Breach violated the provisions of North Dakota Century Code, §51-30-02, requiring Defendant to provide notice of a data security breach to any affected consumers "in the most expedient time possible and without unreasonable delay."

31. Plaintiff fears her Private Information was both stolen in the Data Breach and is still in the hands of the hackers. Plaintiff further believes her Private Information was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals who perpetrate cyberattacks of the type that occurred here.

32. Defendant had obligations created by industry standards, common law, and its own promises and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

33. Plaintiff and Class Members provided their Private Information to medical services providers with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

34. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

35. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[9] Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[10] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[11]

36. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019) University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

37. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[12]

---

[9] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.
[10] *Id*.
[11] *Id*.
[12] FBI, Secret Service Warn of Targeted, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi- secret-service-warn-of-targeted-ransomware (last visited Janu. 25, 2022).

38. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[13]

39. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

DEFENDANT FAILS TO COMPLY WITH FTC GUIDELINES

40. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

41. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[14] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[15]

42. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords

---

[13] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

[14] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 15, 2021).

[15] *Id*.

to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

43. The FTC has brought enforcement actions against businesses for failing to protect patient data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

44. These FTC enforcement actions include actions against healthcare-related service providers like the Defendant. *See, e.g., In the Matter of LabMd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

45. Defendant failed to properly implement basic data security practices.

46. Defendant failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

47. Defendant was at all times fully aware of their obligation to protect the PII of the members of the Class. Defendant was also aware of the significant repercussions that would result from its failure to do so.

DEFENDANT FAILS TO COMPLY WITH INDUSTRY STANDARDS

48. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

49. Several best practices have been identified that at a minimum should be implemented by healthcare service providers like Defendant AHI, including but not limited to educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti- malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

50. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

51. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

52. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

DEFENDANT'S NEGLIGENT ACTS AND BREACH

53. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches;

b. Failing to adequately protect the Private Information of Plaintiff and the Class;

c. Failing to properly monitor their own data security systems for existing intrusions;

d. Failing to train employees in the proper handling of emails containing the means by which the cyberattacks were able to first access Defendant's networks, and to and maintain adequate email security practices;

e. Failing to put into place proper procedures, software settings, and data security software protections to adequately protect against a blunt force intrusion;

f. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and

g. Failing to adhere to industry standards for cybersecurity.

54. As the result of antivirus and malware protection software in need of security updating, inadequate procedures for handling phishing emails or emails containing viruses or other malignant computer code, and other failures to maintain its networks in configuration that would protect against cyberattacks like the one here, Defendant negligently and unlawfully failed to

safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its IT systems and which contained unsecured and unencrypted Private Information.

55. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft.

DATA BREACHES PUT CONSUMERS AT INCREASED RISK OF FRAUD AND IDENTITY THEFT

56. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[16]

57. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into

[16] *See* U.S. Gov. Accounting Office, GAO-07-737, "Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown" (GOA, 2007). Available at https://www.gao.gov/new.items/d07737.pdf. (last visited Jan. 25, 2022).

disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

58. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[17]

59. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

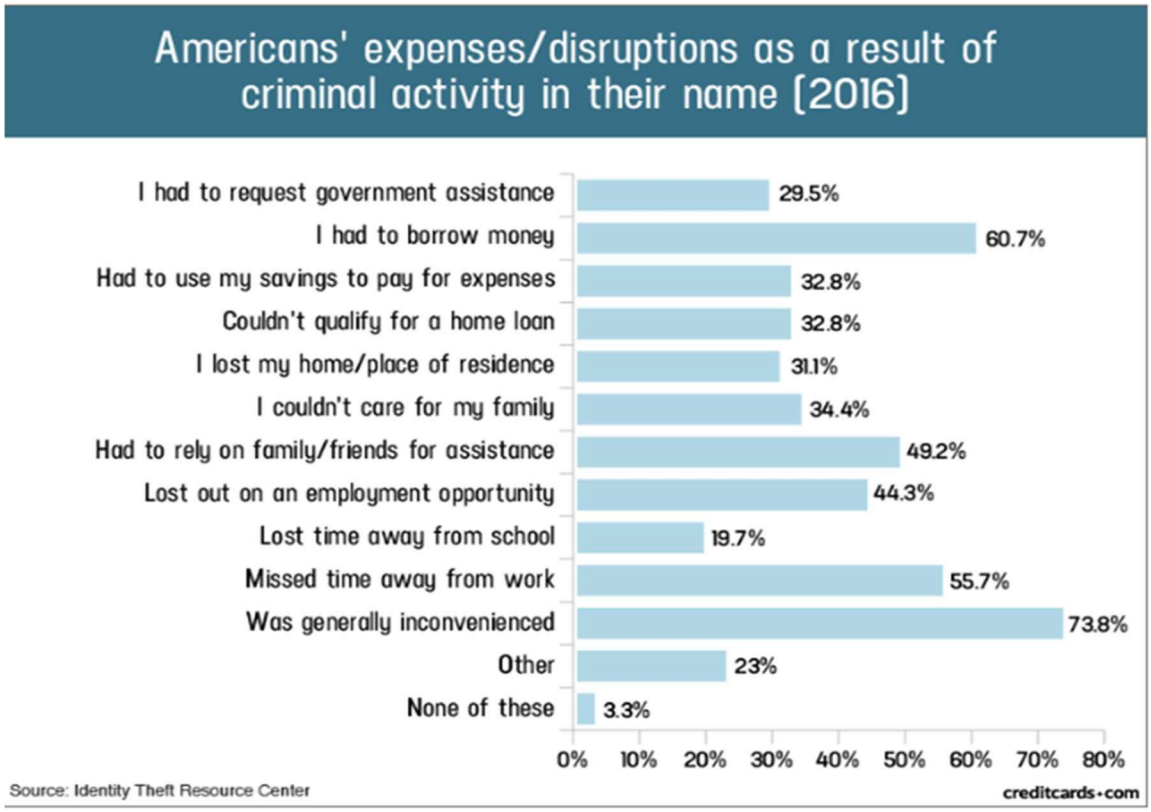
60. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

61. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[18]

---

[17] *See* IdentityTheft.gov, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Jan. 25, 2022).

[18] *See* Jason Steele, Credit Card and ID Theft Statistics, CreditCards.com (Oct. 23, 2020) https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php. (last visited Jan. 25, 2022).



62. Moreover, theft of Private Information is also gravely serious. PII is an extremely valuable property right.[19]

63. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

64. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

---

[19] *See*, e.g., John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

65. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

66. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

67. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

68. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts for many years to come.

69. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[20] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

70. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[21] Such fraud

---

[20] *See* Ashiq Ja, Hackers Selling Healthcare Data in the Black Market, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Jan. 25, 2022).

[21] Identity Theft and Your Social Security Number, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 25, 2022).

may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[22] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

71. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

72. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[23]

73. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[24]

74. For this reason, Defendant knew or should have known about these dangers and strengthened its data, IT, and email handling systems accordingly. Defendant was put on notice

---

[22] *Id*. at 4.

[23] Brian Naylor, Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Jan. 25, 2022).

[24] Tim Greene, Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Jan. 25, 2022).

of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

75. To date, Defendant has done nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

76. Defendant AHI has merely offered Plaintiff and Class Members fraud and identity monitoring services for up to twelve (12) months, but this does nothing to compensate them for damages incurred and time spent dealing with the Data Breach. What is more, Defendant places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

77. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

78. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

79. In or around April 5, 2022, Plaintiff received notice from AHI that her Private Information had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff's Private Information, including name, Social Security number, date of birth, address and telephone number were all compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendant's computer system.

80. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to researching the Data Breach; reviewing credit reports and financial account statements

for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by AHI. Plaintiff now spends approximately one hour per day reviewing her bank accounts and other sensitive accounts for irregularities.

81. As a result of the Data Breach, Plaintiff has suffered emotional distress as a result of the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including increased anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

82. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

83. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

84. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

85. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that AHI obtained from Plaintiff; (b) violation

of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

86. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out- of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

87. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of the Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

V. CLASS ALLEGATIONS

88. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated ("the Class").

89. Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

> All persons whose Private Information was maintained on AHI's system that was compromised in the Data Breach and who were sent a notice of the Data Breach (the "Class").

90. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Also excluded from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

91. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of thousands of individuals whose sensitive data was compromised in the Data Breach.

92. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, e.g., the FTC Act;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Plaintiff and Class Members suffered legally cognizable injuries as a result of Defendant's misconduct;

i. Whether Defendant's conduct was negligent; and

j. Whether Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages, civil penalties, and/or injunctive relief.

93. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

94. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

95. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all of Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

96. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

97. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

VI. CAUSES OF ACTION

COUNT ONE

NEGLIGENCE

98. Plaintiff re-alleges and incorporates by reference the preceding paragraphs above as if fully set forth herein.

99. Companies for which AHI serves as a business associate required its members, including Plaintiff and Class Members, to submit non-public Private Information in the ordinary course of rendering healthcare-related services.

100. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant AHI owed a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft.

101. Defendant AHI owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

102. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

103. As the business associate of a covered entity, Defendant also had a duty under HIPAA privacy laws, which were enacted with the objective of protecting the confidentiality of clients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any business associate of a covered entity.

104. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

105. Defendant also had a duty under N.D. Cent. Code § 51-15-01, *et seq*., to ensure that all customers' medical records and communications were kept confidential.

106. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its IT system;

c. Failing to ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Failure to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' Private Information; and

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

107. It was foreseeable that Defendant AHI failure to use reasonable measures to protect Class Members' Private Information would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

108. It was therefore foreseeable that the failure to adequately safeguard Plaintiff and Class Members' Private Information would result in one or more types of injuries to Class Members.

109. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

110. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant AHI to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide adequate credit monitoring to all Class Members.

COUNT TWO

UNJUST ENRICHMENT

111. Plaintiff re-alleges and incorporates by reference the preceding paragraphs above as if fully set forth herein.

112. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable PII.

113. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff' and Class Members' PII.

114. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

115. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

116. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

117. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

118. Plaintiff and Class Members have no adequate remedy at law.

119. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

120. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

121. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

VII. PRAYER FOR RELIEF

122. WHEREFORE, Plaintiff prays for judgment as follows:

a. or an Order certifying this action as a Class action and appointing Plaintiff and her counsel to represent the Class;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e. Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

f. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

h. Pre- and post-judgment interest on any amounts awarded; and

i. Such other and further relief as this court may deem just and proper.

VIII. JURY TRIAL DEMAND

123. Plaintiff demands a trial by jury on all claims so triable.

DATED: May 12, 2022

Respectfully submitted,

s/David K. Lietz

David K. Lietz
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW
Suite 440
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
dlietz@milberg.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
gklinger@milberg.com

Attorneys for Plaintiff and the Classes

**Pro hac vice forthcoming*